What Is Claimed Is:

1   1.   A method for automatically generating a valid behavior

2   specification for use in an intrusion detection system for a computer system,

3   comprising:

4   receiving an exemplary set of system calls that includes positive examples

5   of valid system calls, and possibly negative examples of invalid system calls; and

6   automatically constructing the valid behavior specification from the

7   exemplary set of system calls by selecting a set of rules covering valid system

8   calls;

9   wherein the set of rules covers all positive examples in the exemplary set

10   of system calls without covering negative examples;

11   wherein selecting a rule for the valid behavior specification involves using

12   an objective function that seeks to maximize the number of positive examples

13   covered by the rule while seeking to minimize the number of possible system calls

14   covered by the rule.

1   2.   The method of claim 1, wherein the objective function additionally

2   seeks to minimize the number of privileged system calls covered by the rule.

1   3.   The method of claim 1, wherein the objective function additionally

2   seeks to minimize a length of the rule.

1   4.   The method of claim 1, wherein the method further comprises

2   monitoring an executing program by:

3   receiving a system call generated by the executing program;

19

1   determining whether the system call is covered by a rule from within the

2   valid behavior specification; and

3   if the system call is not covered by a rule from within the valid behavior

4   specification, indicating that the system call is invalid.

1   5.   The method of claim 1, further comprising producing the

2   exemplary set of system calls by running an exemplary program and recording

3   system calls generated by the exemplary program.

1   6.   The method of claim 1, where the exemplary set of system calls

2   includes calls to functions implemented by an operating system of the computer

3   system.

1   7.   The method of claim 1, wherein the set of rules includes at least

2   one Horn clause.

1   8.   The method of claim 7, wherein selecting a rule for the valid

2   behavior specification involves:

3   selecting a positive example from the exemplary set of system calls;

4   constructing a Horn clause for the positive example by iterating through a

5   subsumption lattice, starting from a most general possible clause and proceeding

6   to a most specific clause for the positive example, and selecting a Horn clause that

7   maximizes the objective function without covering any negative examples;

8   adding the Horn clause to the set of rules in the valid behavior

9   specification; and

20

1   removing other positive examples covered by the Horn clause from the

2   exemplary set of system calls, so subsequently selected Horn clauses do not have

3   to cover the other positive examples.

1   9.   A computer-readable storage medium storing instructions that

2   when executed by a computer cause the computer to perform a method for

3   automatically generating a valid behavior specification for use in an intrusion

4   detection system for a computer system, the method comprising:

5   receiving an exemplary set of system calls that includes positive examples

6   of valid system calls, and possibly negative examples of invalid system calls; and

7   automatically constructing the valid behavior specification from the

8   exemplary set of system calls by selecting a set of rules covering valid system

9   calls;

10   wherein the set of rules covers all positive examples in the exemplary set

11   of system calls without covering negative examples;

12   wherein selecting a rule for the valid behavior specification involves using

13   an objective function that seeks to maximize the number of positive examples

14   covered by the rule while seeking to minimize the number of possible system calls

15   covered by the rule.

1   10.   The computer-readable storage medium of claim 9, wherein the

2   objective function additionally seeks to minimize the number of privileged system

3   calls covered by the rule.

1   11.   The computer-readable storage medium of claim 9, wherein the

2   objective function additionally seeks to minimize a length of the rule.

1   12.   The computer-readable storage medium of claim 9, wherein the

2 method further comprises monitoring an executing program by:

3   receiving a system call generated by the executing program;

4   determining whether the system call is covered by a rule from within the

5 valid behavior specification; and

6   if the system call is not covered by a rule from within the valid behavior

7 specification, indicating that the system call is invalid.

1   13.   The computer-readable storage medium of claim 9, wherein the

2 method further comprises producing the exemplary set of system calls by running

3 an exemplary program and recording system calls generated by the exemplary

4 program.

1   14.   The computer-readable storage medium of claim 9, where the

2 exemplary set of system calls includes calls to functions implemented by an

3 operating system of the computer system.

1   15.   The computer-readable storage medium of claim 9, wherein the set

2 of rules includes at least one Horn clause.

1   16.   The computer-readable storage medium of claim 15, wherein

2 selecting a rule for the valid behavior specification involves:

3   selecting a positive example from the exemplary set of system calls;

4   constructing a Horn clause for the positive example by iterating through a

5 subsumption lattice, starting from a most general possible clause and proceeding

6 to a most specific clause for the positive example, and selecting a Horn clause that

7 maximizes the objective function without covering any negative examples;

1   adding the Horn clause to the set of rules in the valid behavior

2 specification; and

3   removing other positive examples covered by the Horn clause from the

4 exemplary set of system calls, so subsequently selected Horn clauses do not have

5 to cover the other positive examples.

1   17. An apparatus that is configured to automatically generate a valid

2 behavior specification for use in an intrusion detection system for a computer

3 system, comprising:

4   a receiving mechanism that is configured to receive an exemplary set of

5 system calls that includes positive examples of valid system calls, and possibly

6 negative examples of invalid system calls; and

7   a specification construction mechanism that is configured to automatically

8 construct the valid behavior specification from the exemplary set of system calls

9 by selecting a set of rules covering valid system calls;

10   wherein the set of rules covers all positive examples in the exemplary set

11 of system calls without covering negative examples;

12   wherein the specification construction mechanism is configured to select a

13 rule for the valid behavior specification by using an objective function that seeks

14 to maximize the number of positive examples covered by the rule while seeking to

15 minimize the number of possible system calls covered by the rule.

1   18. The apparatus of claim 17, wherein the objective function

2 additionally seeks to minimize the number of privileged system calls covered by

3 the rule.

23

1   19.   The apparatus of claim 17, wherein the objective function

2   additionally seeks to minimize a length of the rule.

1   20.   The apparatus of claim 17, wherein the apparatus further comprises

2   a program monitoring mechanism that is configured to:

3   receive a system call generated by an executing program;

4   determine whether the system call is covered by a rule from within the

5   valid behavior specification; and to

6   indicate that the system call is invalid, if the system call is not covered by

7   a rule from within the valid behavior specification.

1   21.   The apparatus of claim 17, further comprising a trace generation

2   mechanism that is configured to produce the exemplary set of system calls by

3   running an exemplary program and recording system calls generated by the

4   exemplary program.

1   22.   The apparatus of claim 17, where the exemplary set of system calls

2   includes calls to functions implemented by an operating system of the computer

3   system.

1   23.   The apparatus of claim 17, wherein the set of rules includes at least

2   one Horn clause.

1   24.   The apparatus of claim 23, wherein in selecting a rule for the valid

2   behavior specification, the specification construction mechanism is configured to:

3   select a positive example from the exemplary set of system calls;

24

1   construct a Horn clause for the positive example by iterating through a

2 subsumption lattice, starting from a most general possible clause and proceeding

3 to a most specific clause for the positive example, and selecting a Horn clause that

4 maximizes the objective function without covering any negative examples;

5   add the Horn clause to the set of rules in the valid behavior specification;

6 and to

7   remove other positive examples covered by the Horn clause from the

8 exemplary set of system calls, so subsequently selected Horn clauses do not have

9 to cover the other positive examples.

25